

**FILED****United States District Court**

DEC - 6 2005

MIDDLE

DISTRICT OF

ALABAMA

CLERK

U. S. DISTRICT COURT  
MIDDLE DIST. OF ALA.**In the matter of the Search of**(Name, address or brief description of person, property or premises  
to be searched)**APPLICATION AND AFFIDAVIT  
FOR SEARCH WARRANT**

Yahoo!, Inc.

701 First Avenue, Sunnyvale, CA 94089

Contents of e-mail account:

bebitzaa@yahoo.com

CASE NUMBER: 2:05mj146-W

I MICHAEL P. EUBANKS

being duly sworn depose and say:

I am a(n) Special Agent, Federal Bureau of Investigation and have reason to believethat ☐ on the person of or ☒ on the property or premises known as (name, description and/or location)

Yahoo!, Inc., 701 First Avenue, Sunnyvale, CA 94089

Contents of e-mail account: bebitzaa@yahoo.com

in the Northern District of California

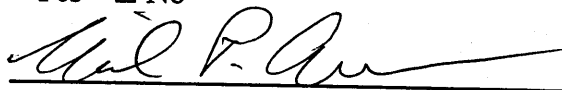
there is now concealed a certain person or property, namely (describe the person or property to be seized)

**See Attachment A**

which is (state one or more bases for search set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

**contraband or property that constitutes evidence of the commission of a criminal offense,**concerning a violation of Title 18 United States Code, Section(s) 1343 & 2320.

The facts to support the issuance of a Search Warrant are as follows:

**See Attached Affidavit**Continued on the attached sheet and made a part hereof: ☒ Yes ☐ No

Signature of Affiant

Sworn to before me and subscribed in my presence,

November 2, 2005 12:10pm at Montgomery, Alabama

Date

City and State

SUSAN RUSS WALKER, U.S. Magistrate Judge

Name &amp; Title of Judicial Officer



Signature of Judicial Officer

AFFIDAVIT

I, MICHAEL P. EUBANKS, being duly sworn depose, say, and provide the following information (obtained by me unless otherwise noted):

I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been assigned to the Mobile, Alabama Division of the FBI since April, 1999. As a Special Agent of the FBI, I am authorized to investigate crimes involving computer fraud and conspiracies to commit those crimes. I have a Master of Science Degree in Software Systems Engineering, a Bachelor of Science Degree in Computer Science, and approximately seven years of professional experience as a computer programmer in private industry. Additionally, I have received special training relevant to the investigation of computer related crimes including courses in network security, advanced computer intrusion investigations, and computer network exploitation.

I am familiar with the information contained in this affidavit from information provided to me in the form of written and oral reports made by other FBI Agents, by victim and witness interviews, through e-mail correspondence with Region's Bank information technology and security personnel, by evidence discovered from information returned from Grand Jury subpoenas, discussions with computer experts, and public source information available on the Internet.

This affidavit is offered in support of an application for a search warrant for one e-mail account

1 controlled by the free web-based electronic mail service  
2 provider known as Yahoo!, Inc. ("Yahoo!"), headquartered at  
3 701 First Avenue, Sunnyvale, California 94089. The account to  
4 be searched is **bebitzaa@yahoo.com**, which is further described  
5 in the following paragraphs and in Attachment A. As set forth  
6 herein, there is probable cause to believe that on the  
7 computer systems of Yahoo!, there exists evidence, fruits,  
8 and instrumentalities of the violations of Title 18, United  
9 States Code, Section 1343, wire fraud and Title 18, United  
10 States Code, Section 2320, trafficking in counterfeit goods  
11 or services.

12 In my training and experience, I have learned that  
13 Yahoo! is a company that provides free web based Internet  
14 electronic mail ("e-mail") access to the general public, and  
15 that stored electronic communications, including opened and  
16 unopened e-mail for Yahoo! subscribers may be located on the  
17 computers of Yahoo!. Further, I am aware that computers at  
18 Yahoo! contain information and other stored electronic  
19 communications belonging to third parties. Accordingly, this  
20 affidavit and application for search warrant seek  
21 authorization solely to search the computer accounts and/or  
22 files and following the procedures described herein and in  
23 Attachment A.

24 Pursuant to Title 18, United States Code, Section  
25 2703(c)(1)(A), "A governmental entity may require a provider  
26 of electronic communication service or remote computing  
27 service to disclose a record or other information pertaining  
28 to a subscriber to or other information pertaining to a

1 subscriber to or customer of such service (not including the  
2 contents of communications) only when the governmental agency  
3 obtains a warrant issued using the procedures described in  
4 the Federal Rules of Criminal Procedure by a court with  
5 jurisdiction over the offense under investigation..."

6 Search Procedure

7 In order to ensure that agents search only those  
8 computer accounts and/or files described herein and in  
9 Attachment A, this affidavit and application for search  
10 warrant seeks authorization to permit employees of Yahoo! to  
11 assist agents executing this warrant to search only those  
12 computer accounts and/or files described in Attachment A, the  
13 following procedures will be implemented:

- 14 1. The search warrant will be presented to Yahoo!  
15 personnel who will be directed to isolate  
16 those accounts and files described in  
17 Attachment A;
- 18 2. In order to minimize any disruption of  
19 computer service to innocent third parties,  
20 Yahoo! employees trained in the operation of  
21 computers will create an exact duplicate of  
22 the computer accounts and files described  
23 below, including an exact duplicate of all  
24 information stored in the computer accounts or  
25 files described below;
- 26 3. Yahoo! personnel will provide the exact  
27 duplicate of the accounts and files described  
28 below, and all information stored in those

1 accounts and/or files to the Special Agent who  
2 serves this search warrant;

- 3 4. Law enforcement personnel will thereafter  
4 review the information stored in the accounts  
5 and files received from Yahoo! for evidentiary  
6 purposes.

7 **Background regarding Computers, the Internet, and E-Mail**

8 The term "computer" as used herein is defined in 18  
9 U.S.C. Section 1030(e)(1), and includes and electronic,  
10 magnetic, optical, electrochemical, or other high speed data  
11 processing device performing logical, arithmetic, or storage  
12 functions, and includes any data storage facility or  
13 communications facility directly related to or operating in  
14 conjunction with such device.

15 I have had both training and experience in the  
16 investigation of computer-related crimes. Based on my  
17 training, experience, and knowledge, I know the following:

- 18 1. The Internet is a worldwide network of  
19 computer systems operated by governmental  
20 entities, corporations, and universities. In  
21 order to access the Internet, an individual  
22 computer user must subscribe to an access  
23 provider, which operates a host computer  
24 system with direct access to the Internet. The  
25 World Wide Web ("www") is a functionality of  
26 the Internet which allows users of the  
27 Internet to share information;

- 28 2. With a computer connected to the Internet, an

1 individual computer user can make electronic  
2 contact with millions of computers around the  
3 world. This connection can be made by any  
4 number of means, including modem, local area  
5 network, wireless and numerous other methods;

- 6 3. E-Mail is a popular form of transmitting  
7 messages and/or files in an electronic  
8 environment between computer users. When an  
9 individual computer users sends e-mail, it is  
10 initiated at the user's computer, transmitted  
11 to the subscriber's mail server, then  
12 transmitted to its final destination. A server  
13 is a computer that is attached to a dedicated  
14 network and serves many users. An e-mail  
15 server may allow users to post and read  
16 messages and to communicate via electronic  
17 means.

18 **Yahoo! Mail**

19 Based on my training and experience, I have learned  
20 the following about Yahoo! Mail:

- 21 1. Yahoo! Mail is an e-mail service which offers  
22 e-mail accounts free of charge to Internet  
23 users. Subscribers obtain an account by  
24 registering on the Internet at the Yahoo! web  
25 site (www.yahoo.com). Yahoo! requests  
26 subscribers to provide basic information, such  
27 as name, address, zip code, and phone.  
28 However, Yahoo! does not verify the

1 information provided;

2 2. Yahoo! maintains electronic records pertaining  
3 to the individuals and companies for which  
4 they maintain subscriber accounts. These  
5 records include account access information, e-  
6 mail transaction information, and account  
7 application information;

8 3. Subscribers to Yahoo! Mail may access their  
9 accounts on servers maintained and/or owned by  
10 Yahoo! from any computer connected to the  
11 Internet located anywhere in the world;

12 4. Any e-mail that is sent to a Yahoo! subscriber  
13 is stored in the subscriber's "mail box" on  
14 Yahoo!'s servers until the subscriber deletes  
15 the e-mail or the subscriber's mailbox exceeds  
16 the storage limits preset by Yahoo!. If the  
17 message is not deleted by the subscriber, the  
18 account is below the maximum limit, and the  
19 subscriber accesses the account periodically,  
20 that message can remain on Yahoo!'s servers  
21 indefinitely;

22 5. When the subscriber sends an e-mail, it is  
23 initiated at the user's computer, transferred  
24 via the Internet to Yahoo!'s servers, and then  
25 transmitted to its end destination. Yahoo!  
26 users have the option of saving a copy of the  
27 e-mail sent. Unless the sender of the e-mail  
28 specifically deletes the e-mail from the

1 Yahoo! server, the e-mail can remain on the  
2 system indefinitely. The sender can delete  
3 the stored e-mail message thereby eliminating  
4 it from the e-mail box maintained at Yahoo!,  
5 but that message will remain in the  
6 recipient's e-mail box unless the recipient  
7 deletes it as well or unless the recipient's  
8 account is subject to account size  
9 limitations;

- 10 6. A Yahoo! subscriber can store files, including  
11 e-mails and image files, on servers maintained  
12 and/or owned by Yahoo!;
- 13 7. E-mails and image files stored on a Yahoo!  
14 server by a subscriber may not necessarily be  
15 located in the subscriber's home computer.  
16 The subscriber may store e-mails and/or other  
17 files on the Yahoo! server for which there is  
18 insufficient storage space in the subscriber's  
19 computer and/or which he/she does not wish to  
20 maintain in the computer in his/her residence.  
21 A search of the files in the computer in the  
22 subscriber's residence will not necessarily  
23 uncover the files that the subscriber has  
24 stored on the Yahoo! server.

25  
26 **Probable Cause**

27 This investigation was initiated on February 17,  
28 2005 after security personnel at Region's Bank contacted the

1 FBI to report numerous solicitations by unknown, unauthorized  
2 person(s) for Regions's Bank customer information via the  
3 Internet. A particular solicitation which occurred on April  
4 29, 2005 is the primary focus of this affidavit.

5  
6 **Internet "Phishing" Background**

7 The technique utilized by the unauthorized  
8 person(s) in this investigation is known as Internet  
9 "phishing". "Phishing" is conducted by an unauthorized user  
10 who creates an Internet web site which is either a clone of  
11 an original Internet web site or else is a customized web  
12 site which utilizes counterfeit marks in an effort to appear  
13 as if it a site which belongs to the company or organization  
14 being targeted in the scheme. After the creation of the web  
15 site, the perpetrator conducts an unlawful computer intrusion  
16 and obtains access to a computer system on which the  
17 counterfeit web site can be hosted for viewing by all  
18 Internet users. Once the web site is running on the victim  
19 computer system, the perpetrator uses a variety of  
20 techniques to make the website appear authentic, including  
21 creating a web site name which closely resembles that of the  
22 authentic site. Potential users of the authentic website are  
23 then identified through targeted e-mail "harvesting" from the  
24 Internet. Mass e-mail solicitation is then performed in an  
25 effort to direct these potential victims to the cloned web  
26 site where they are requested to provide specific financial  
27 information. Once obtained by the perpetrators, this  
28 financial information is then abused for their own financial

1 gain.

2           The victims in Internet "phishing" schemes include  
3 the targeted corporation for which the counterfeit web site  
4 created, the targeted recipients of the mass e-mail  
5 solicitations whom respond to the "phishing" e-mail, and the  
6 corporation or person whose computer was used to host the  
7 counterfeit web site.

8           Region's Bank began experiencing "phishing" attacks  
9 in large numbers during November 2004. Region's Bank has  
10 been the victim of at least 735 identified "phishing" web  
11 sites and has incurred direct financial losses of  
12 \$1,424,955.61 in responding to these "phishing" web sites  
13 since November 2004. This loss is quantified through the  
14 time devoted by Information Technology personnel responding  
15 to each "phishing" attack. Response includes time devoted by  
16 personnel in negotiating the removal of the web site from the  
17 Internet and costs to the bank for contracting experts in the  
18 removal of such sites. This does not include the loss to the  
19 solicited victims of each "phish" or to the victim company  
20 where the intruder hosted the "phishing" web site. Evidence  
21 from computers on which the counterfeit "phishing" web site  
22 was hosted is difficult to obtain since these computers are  
23 often located throughout the world and are only active for  
24 short periods of time.

25           **"Phishing" Incident on April 29, 2005**

26           During the course of this investigation, Region's  
27 Bank Information Technology personnel discovered a "phishing"  
28 website on approximately May 6, 2005 and forwarded the

1 Internet address to the FBI. This Internet address was  
2 identified as the following: [http://regionsnet-](http://regionsnet-update.darakonbd.com/wn/.https/sslregions/cmserver/EBanking/1)  
3 [update.darakonbd.com/wn/.https/sslregions/cmserver/EBanking/1](http://regionsnet-update.darakonbd.com/wn/.https/sslregions/cmserver/EBanking/1)  
4 [ogon/user.htm](http://regionsnet-update.darakonbd.com/wn/.https/sslregions/cmserver/EBanking/1). See Attachment B. Internet users who  
5 received the mass solicitation were fraudulently advised  
6 through an e-mail that Region's Bank was conducting a  
7 security update and the users were requested to provide for  
8 verification purposes the following information for their  
9 Region's Bank accounts: ATM or debit card information, ATM  
10 PIN number, CVV Number for the credit card, and card  
11 expiration date. CVV stands for 'card verification value'.  
12 The CVV number is a three or four digit authentication code  
13 on a credit card in addition to the card number. It is used  
14 as an anti-fraud security feature that a merchant would ask  
15 for to help verify that the cardholder actually has  
16 possession of the credit card.

17 FBI personnel working at the National Cyber  
18 Forensic and Training Alliance (NCFTA), a joint computer  
19 crime task force based in Pittsburgh, Pennsylvania, conducted  
20 research into the above described cloned Region's Bank web  
21 site and discovered it was being hosted on a computer in the  
22 country of Austria. An analyst at the NCFTA was able to gain  
23 access to a directory on the hosting computer in Austria  
24 through an Internet browser and a short computer program was  
25 discovered which collected the requested information and  
26 forwarded it to the e-mail address **bebitzaa@yahoo.com**. This  
27 information was provided to the FBI Office in Mobile, Alabama  
28 for further investigation.

1           On May 19, 2005, a Grand Jury subpoena from the  
2 Middle District of Alabama for information on the  
3 **bebitzaa@yahoo.com** account was issued and sent to Yahoo!.  
4 The return results revealed that the account was created on  
5 January 26, 2005 and had been accessed by a user 304 times  
6 between February 15, 2005 and May 30, 2005. All 304 accesses  
7 were traceable to four specific computers with Internet  
8 addresses in the country of Romania.

9           On June 29, 2005 a communication was sent to the  
10 FBI Legal Attache in Bucharest, Romania with instructions to  
11 disseminate the analyzed information regarding the traced e-  
12 mail accesses to Romanian Law Enforcement personnel.  
13 Romanian Officials were further requested to determine if the  
14 Internet addresses of the computers were traceable to a  
15 specific residence or business.

16           On October 12, 2005, the FBI Legal Attache in  
17 Bucharest, Romania received a translated copy of a letter  
18 from Romanian Police that several of the Internet accesses  
19 connected to the **bebitzaa@yahoo.com** e-mail account were  
20 allocated to SIMONA VALEANU and DINU CIUHIA, both in Suceava,  
21 Romania. During late September, 2005 Officer BOGDAN UDREA of  
22 the Romanian Police spoke with Special Agent Michael Eubanks  
23 of the Mobile Office of the FBI and advised if more  
24 information could be provided regarding the  
25 **bebitzaa@yahoo.com** e-mail account, the Romanian Police may  
26 have enough probable cause to conduct a search of the  
27 computer at the identified residence and to interview the  
28 owner of the computer to determine their involvement in the

"phishing" scheme.

Conclusion

Based on the information above, your affiant believes that on the computer systems owned, maintained, and/or operated by Yahoo!, Inc., headquartered at 701 First Avenue, Sunnyvale, California 94089, there exists evidence, fruits, and instrumentalities of violations of Title 18, U.S.C., Section 1343 and Title 18, U.S.C. Section 2320. By this affidavit and application, I request that the Court issue a search warrant directed at Yahoo! allowing agents to seize the e-mail and other information stored on the Yahoo! servers for the computer accounts and files and following the search procedure described in Attachment A.



Michael P. Eubanks  
Special Agent  
Federal Bureau of Investigation  
Mobile, Alabama

Subscribed and sworn to before me this 2nd day of November, 2005



Susan Russ Walker  
U.S. Magistrate Judge

**Attachment A**

**A. Search Procedure**

In order to ensure that agents search only those computer accounts or computer files described in Attachment A, this search warrant seeks authorization to permit employees of Yahoo!, Inc. to assist agents in the execution of this warrant. To further ensure that agents executing this warrant search only those accounts or computer files described in Attachment A, the following procedures have been implemented:

1. The warrant will be presented to Yahoo! personnel who will be directed to isolate those accounts and files described in Attachment A;
2. In order to minimize any disruption of computer service to innocent third parties, the systems administrator will create an exact duplicate of the accounts and files described in Attachment A, including an exact duplicate of all information stored in the computer accounts or files described in Attachment A;
3. Yahoo! personnel will provide the exact duplicate of the accounts and files described in Attachment A and all information stored in those accounts and/or files to the Special Agent who serves this search warrant;
4. Law enforcement personnel will thereafter review the information stored in the accounts and files received from Yahoo! and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant;
5. Law enforcement personnel will then seal the original duplicate of the accounts and files received from the systems administrator and will not further review the original duplicate absent an order of the Court; and

**B. Description of Accounts and Computer Files to be Copied by Yahoo!, Inc.**

All electronic mail stored and presently contained in, or on behalf of, the following email address or individual account: **bebitzaa@yahoo.com.**

1. Printouts of all of the above from original storage.
2. Any and all transactional information, to include log files, of all activity to the above-listed individuals which includes dates, time, method of connecting, port, dial-up, and/or location, including source IP address(es) and destination IP address(es) of any and all e-mails sent or received by the Yahoo! account names

**bebitzaa@yahoo.com.**

3. All business records and subscriber information, in any form kept, which pertain to the above listed subscribers and accounts, including but not limited to applications, subscribers' full names, all screen names associated with those subscribers and accounts, all account names associated with those subscribers, method of payment, phone numbers, addresses, and detailed-billing records.

**C. Description of Information to be Further Copied by Law Enforcement Personnel**

1. All communications within the email account of **bebitzaa@yahoo.com** that:
  - a. are to or from or refer to the email account **bebitzaa@yahoo.com**.
  - b. refer to interstate or international travel.
2. All items identified in section B, paragraph 2, of this attachment that relate to those communications identified as being described in section C, paragraphs 1 and 2, of this Attachment.
3. All items identified in section B, paragraph 3, of this Attachment.

Any communications or files which can be provided in electronic format (ie: CD) would be preferable, if at all possible.

END OF ATTACHMENT

**Regions NET**

Please enter the requested information below.

By resuming to this process, system you agree to have read and accepted the terms set forth in the Regions Online Member Agreement and Disclosure Statement.  
 \* = Required Field

RegionBank ATM or Debit Card Number:  
 RegionBank ATM PIN Number:  
 Cvv Number:  
 Card Exp. Date:

[Redacted]

ATTACHMENT B